

39524223

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Serial No.
Filing Date
Inventorship Venkatesan et al
Applicant Microsoft Corporation
Attorney's Docket No. MS1-1922US
Title: Primitives for Fast Secure Hash Functions and Stream Ciphers

INFORMATION DISCLOSURE STATEMENT

References -- See Attached Form PTO-1449

REMARKS

The citations listed, copies attached, are submitted in compliance with the duty of disclosure defined in 37 CFR §1.56. The Examiner is requested to make these citations of official record in this application.

Respectfully Submitted,

Date: 2/9/04

By: Ramin Aghevi
Ramin Aghevi
Reg. No. 43,462

EV 395542223 +

Substitute for form 1449A/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(use as many sheets as necessary)</i>				Complete if Known	
				Application Number	
				Filing Date	
				First Named Inventor	Venkatesan
				Group Art Unit	
				Examiner Name	
Sheet	1	of	3	Attorney Docket Number	MS1-1922US

U.S. PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code ² (if known)			
		6,496,928		Deo et al	12-17-2002	
		6,275,599		Adler et al	08-14-2001	
		5,673,316		Auerback et al	09-30-1997	
		5,651,069		Rogaway	07-22-1997	
		3,962,539		Ehrsam et al.	06-08-1976	
		4,200,770		Hellman et al.	04-29-1980	
		4,218,582		Hellman et al.	08-19-1980	
		4,309,569		Merkle	06-05-1982	
		4,405,829		Rivest et al.	08-20-1983	
		4,625,076		Okamoto et al.	11-25-1986	
		4,748,668		Shamir et al.	05-31-1988	
		4,850,017		Matyas, Jr. et al	07-18-1989	
		4,850,019		Shimizu et al.	07-18-1989	
		4,908,861		Bracht et al.	03-13-1990	
		4,995,082		Schnorr	02-19-1991	
		5,140,634		Guillou et al	08-18-1992	
		5,214,703		Massey et al	05-25-1993	
		5,231,668		Kravitz	07-27-1993	
		5,276,737		Micali	01-04-1994	
		3,798,359		Feistel	03-19-1974	

[illegible]

Examiner Signature		Date Considered	
-----------------------	--	--------------------	--

¹ Unique citation designation number. ² See attached Kinds of U.S. Patent Documents. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U. S. Patent and Trademark Office, Washington, DC 20231. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO:** Assistant Commissioner for Patents, Washington, DC 20231.

+

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U. S. Patent and Trademark Office, Washington, DC 20231. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO:** Assistant Commissioner for Patents, Washington, DC 20231.

Please type a plus sign (+) inside this box → +

95542223

+

<div>Substitute for form 1449B/PTO</div> <div>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</div> <div>(use as many sheets as necessary)</div>				Complete if Known		
Sheet		3	of	3	Application Number	
					Filing Date	
					First Named Inventor	Venkatesan
					Group Art Unit	
					Examiner Name	
					Attorney Docket Number	MS1-1922US

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
		MENEZES, A., van OORSCHOT, P., and VANSTONE, S.; Chapter 9, "Hash Functions and Data Integrity" from Handbook of Applied Cryptography CRC Press 1996 pgs 321 to 383	
		MENEZES, A., van OORSCHOT, P., and VANSTONE, S.; Chapter 6, "Stream Ciphers" from Handbook of Applied Cryptography CRC Press 1996 pgs 321 to 383	
		BENJAMINI, I., BERGER, N., HOFFMAN, C., MOSSEL, E.; "Mixing Times of the Biased Card Shuffling and the Asymmetric Exclusion Process" Submitted for Publication October 9, 2002 22 pages	
		MIRONOV, ILYA; "(Not So) Random Shuffles of RC4" Advances in Cryptology, CRYPTO 2002, 19 pages	
		MANTIN, ITSIC; "RC4 Webpage" http://www.wisdom.weizmann.ac.il/~itsik/RC4/rc4.html 2 pages	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Unique citation designation number. ² Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U. S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.